DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET // SI / TK // REL TO USA AUS CAN GBR NZL

(U//FOUO) Interview with a SID ''Hacker'' -- Part 1: How Does TAO Do Its Work?

FROM: [redacted] the SIDtoday Editor

Run Date: 07/12/2012

[redacted]

(S//REL) One organization that has grown substantially in recent years is Tailored Access Operations (S32), the group that hacks our targets'

computers. [redacted] (pictured), a counterterrorism subject-matter expert in TAO's Requirements and Targeting organization, spoke with SID*today* recently to explain how TAO carries out its work:

---

1. (U//FOUO) What do TAO Requirements & Targeting analysts like you do? -- What's your role?

(U) Our role in R&T is to serve as a liaison with the TOPIs in S2. We work with the TOPIs to find out what they really want in terms of CNE [computer-network exploitation] collection and then work within TAO to figure out how to get it... To give you a quick overview, there are different elements in TAO:

- (U//FOUO) First there are are the ***developers*** who create the software and the hardware -- the tools that TAO uses to carry out our collection.
- (U//FOUO) Next are the ***operators*** in the ROC [Remote Operations Center] who actually ***use*** the tools. They do the actual collection of intelligence from the targets' systems, while showing good OPSEC [operations security] and making sure our tools themselves are protected.
- (U//FOUO) And then there is my element, Requirements and Targeting. We are the ***analysts and planners*** for operations. We find out what the TOPIs are looking for, do the network analysis, and draw up a plan for getting that collection.
- (U//FOUO) Supporting it all are the folks who provide the infrastructure. They provide the computers, networks, etc. and keep everything running.

(U//FOUO) Each group brings a different skill to the table. Regarding the tools we use, the developers know the ***coding*** for them, the operators know ***how to use*** them, and R&T just ***knows that they exist***. R&T's focus is on ***where we can apply*** the tools to get the intelligence we want.

(U//FOUO) In TAO, we all have to work hand-in-glove. Often the analysts are eager to grab whatever intelligence we can, while the operators are more conscious of the risks involved, so we meet somewhere in between. Each side brings their own perspective and it creates checks and balances.

(U//FOUO) The ROC does after-action reviews of operations -- every action taken is automatically recorded -- to make sure things were done appropriately. Operators have to be certified -- and they can have their certifications pulled -- so they have a strong incentive to show good OPSEC.

2. (U//FOUO) Do R&T analysts participate when operations are carried out in the ROC? If so, how does it play out?

(U//FOUO) Yes, the R&T analysts actually sit side-by-side with the ROC operators when an operation takes place. We're there to provide ***knowledge of the networks***, and the operators, as I mentioned, know how to ***use the tools*** to extract the data.

(U//FOUO) Nowadays there are dedicated analysts and operators working on

specific targets. So, for example, I work the CT [counterterrorism] target, and we have counterpart operators who focus on CT, too. (In the past, we analysts would have shown up for an operation and been assigned an operator randomly out of a pool.) The benefit of this new approach is that the analysts and operators can develop working relationships and collaborate ahead of time on an upcoming operation.

(U//FOUO) In terms of how an operation is scheduled, our analysts decide to work a project and start to do research on targets to go after. Next we get approvals through the ROC mission directors to pursue operations against those targets. The mission directors are a small group of people with lots of experience. They assess the risks involved in the operation and approve or deny it. Once we have the approval, the analysts plan an operation in coordination with an operator and, when they are ready, arrange a specific time to carry it out. We have the flexibility to conduct the operation at the optimal time.

(U//FOUO) In the early days TAO used to be just a bunch of hackers! We did things in a more ad hoc manner... one guy did it all. Now we're more systematic in how we do things.

(S//SI//REL) In the CT world, we usually go after the infrastructure (like an ISP [internet service provider]) or after the specific target in end-point collection -- extracting data from a specific "box" [computer or device]. Normally collection is automated for end-point, but sometimes it's an interactive, real-time event when the target is up on the net. The latter happens quite a bit in CT. The operations might take place at 2AM or 6AM, since that is when the target is active. Some CT targets use really slow dial-up connections from remote places in the Pakistani tribal areas, and we have to move quickly when the opportunity presents itself.

(U) ...Do you need linguists to participate in your operations, to translate the names of the files, etc?

(S//SI/REL) Not as much as you might think. We don't evaluate the content of the data, we just collect it. Usually we have an idea of what types of files and information the TOPIs are interested in -- like text files -- and we try to grab all of it for analysis later. We don't take the time during the operation to sort out the good from the bad.

(U) Stand by for the conclusion of this interview., appearing tomorrow. [Editor's note: click HERE.]

NSANet without the consent of S0121